

Learner Data Privacy

Problem Statement. *Privacy is a central concern in the Information Age, and data-privacy considerations affect many aspects of learning and development (e.g., training and education systems, career planning, learner profiles, skills assessments). Given that data-rich systems can provide added value to learning and development, as well as workforce planning, how should system owners maximize the utility of data while also treating personal information responsibly?*

Background: “Privacy by Design” is a user-centered philosophy in which privacy aspects are addressed early in the design and development process. From 2016–2019, the ADL Initiative sponsored research on learner data privacy within the context of the Total Learning Architecture (TLA).¹ This project resulted in prototype concepts, early requirements, and a review of applicable DoD and federal government policies. The project also produced the initial foundations for a Privacy API that would allow individuals to modify their privacy settings once and then propagate those settings to other connected systems.



Outcomes: This research builds on the ADL Initiative’s TLA and learner privacy research, and relates to the FY20 Universal Learner Records research topic. This project will first **validate the prior research recommendations** against existing policy and best practices. Then it will produce **requirements and specifications for an iteration of a Privacy API** that can function within the TLA. The specifications and other design documentation should address all standard component-types within a learning environment (e.g., edge systems, such as learning management systems, and central systems, such as universal learner records). These documents should also consider how data are handled at different organizational levels (e.g., immediate data within a given learning instance, data aggregated across several months at a school, career-spanning data aggregated at the enterprise level², etc.), and they should inform questions such as: Where should different kinds of data reside, who owns what data, how should different portions of a dataset be used or shared, and how should federated applications negotiate for data access and reuse? Next, the project will deliver a **reference implementation of the Privacy API**, integrated into existing tools, learning activities, and/or other TLA components in a sandbox environment. (Note, other government engineers or contracted performers may be asked to implement the Privacy API based upon its documentation.) Finally, the developers will **test and demonstrate** the prototype, including tests of its functional and nonfunctional requirements (e.g., user experience).

Note: Privacy best practices are influenced by the General Data Protection Regulation (GDPR), a legal framework for handling personal information in the European Union. This project should examine GDPR recommendations.

| Summary of Major Objectives | Associated Deliverables |
|--|--|
| Baseline DoD privacy policies and requirements | Privacy report and guidance (based on prior research) |
| Collect/analyze requirements for Privacy API | Requirements and other design documentation |
| Author design documents | Architectural design and software design documents |
| Develop prototype reference implementation | Documentation and implementation of prototype API |
| Test/demonstrate Privacy API prototype | Successful demonstration and functional testing report |
| Author privacy roadmap and recommendations | Policy recommendations report for DoD/Government |
| Author ready-to-use Privacy API documentation | Documentation for developers and system administrators |

¹ Refer to the “Privacy Support for the Total Learning Architecture (PS4TLA)” project, <https://adlnet.gov/ps4tla>

² See Gordon, J. (2019, June) Talent Development Toolkit Requirements and Architecture, Version 1.0. Refer to the section on Control Loops.